Multiplicative character sums and products of sparse integers in residue classes

Ostafe, Alina ; Shparlinski, Igor E

Abstract: We estimate multiplicative character sums over the integers with a fixed sum of binary digits and apply these results to study the distribution of products of such integers in residues modulo a prime p. Such products have recently appeared in some cryptographic algorithms, thus our results give some quantitative assurances of their pseudorandomness which is crucial for the security of these algorithms

DOI: https://doi.org/10.1007/s10998-012-6771-2

Periodica Mathematica Hungarica Vol. 64 (2), 2012, pp. 247–255
DOI: 10.1007/s10998-012-6771-2

MULTIPLICATIVE CHARACTER SUMS AND PRODUCTS OF SPARSE INTEGERS IN RESIDUE CLASSES

Alina Ostafe[1] and Igor E. Shparlinski[2]

[1]Institut für Mathematik, Universität Zürich
Winterthurerstrasse 190, Zürich, CH-8057, Switzerland
E-mail: alina.ostafe@math.uzh.ch

[2]Department of Computing, Macquarie University
Sydney, NSW 2109, Australia
E-mail: igor.shparlinski@mq.edu.au

(*Received July 28, 2010; Accepted September 22, 2010*)

[Communicated by András Sárközy]

Abstract

We estimate multiplicative character sums over the integers with a fixed sum of binary digits and apply these results to study the distribution of products of such integers in residues modulo a prime p. Such products have recently appeared in some cryptographic algorithms, thus our results give some quantitative assurances of their pseudorandomness which is crucial for the security of these algorithms.

1. Introduction

Let $\sigma(n)$ denote the sum of binary digits of n; that is,

$$\sigma(n) = \sum_{j \ge 0} a_j(n),$$

where

$$n = \sum_{j \ge 0} a_j(n) 2^j, \qquad a_j(n) = 0, 1.$$

For any integers $0 \le s \le r$, let

$$\mathcal{G}_s(r) = \{0 \le n < 2^r \mid \sigma(n) = s\}.$$

Mathematics subject classification numbers: 11A63, 11L40, 11T71.
Key words and phrases: character sums, congruences, sparse integers.

0031-5303/2012/$20.00

Akadémiai Kiadó, Budapest
Springer, Dordrecht

Then $\mathcal{G}_s(r)$ is the set of integers with r digits (in base 2) such that the sum of the digits is equal to s.

Let p be a fixed prime number. Some exponential and character sums over the integers from the set $\mathcal{G}_s(r)$ and some other sets of integers with restricted digits have been considered in [1], [3]. In this paper, we establish nontrivial bounds for character sums of the form

$$S_s(r, \chi, f) = \sum_{n \in \mathcal{G}_s(r)} \chi(f(n)),$$

where χ is a non-principal multiplicative character of the finite field $\mathbb{F}_p$ with p elements, and $f(X)$ is a polynomial in $\mathbb{F}_p[X]$. Our results apply only to linear polynomials f improving those of [1] established for arbitrary polynomials and are based on an estimate of incomplete character sums with polynomials, which follows from the Weil bound for mixed sums of multiplicative and additive characters [7].

In order to simplify our calculations and the formulation of our main results, we consider only the case where the prime p is greater than 2^r; however, our methods and results can be extended to cover smaller values of p as well. Moreover, we remark that the most challenging and interesting problem is to obtain nontrivial bounds when the value of 2^r is about p but s is as small as possible.

Besides being of intrinsic interest, bounds of such sums can also be used to study the distribution of products of integers from the sets $\mathcal{G}_s(r)$. Questions of this kind are motivated by recently suggested algorithms of fast exponentiation [2], [4], as a part of some cryptographic protocols. Thus, establishing the uniformity of distribution of such products (which can be rephrased in terms of their pseudo-randomness and entropy) is important for giving some security assurances of these protocols.

For our bounds to be nontrivial, the set $\mathcal{G}_s(r)$ must be of sufficiently large cardinality, however, it applies to sparse integers (that is, to smaller values of s) than a more general result of [1].

2. Preparations

Throughout the paper, the implied constants in the symbols "O" and "$\ll$" may depend on an integer parameter $\nu \geq 1$. We recall that the expressions $A \ll B$ and $A = O(B)$ are each equivalent to the statement that $|A| \leq cB$ for some constant c. As usual, $\log z$ denotes the natural logarithm of z.

We now recall that

$$\#\mathcal{G}_s(r) = \binom{r}{s} = 2^{rH(s/r)+o(r)},$$

where

$$H(\gamma) = \frac{-\gamma \log \gamma - (1-\gamma)\log(1-\gamma)}{\log 2}$$

denotes the *binary entropy function*, see [5, Section 10.11].

We need the following elementary statement:

LEMMA 1. *For any reals γ and τ with $0 < \gamma\tau < 1$ and $\tau > 1$, we have*

$$H(\gamma\tau) < \tau H(\gamma).$$

PROOF. It is easy to check that

$$\frac{dH(\gamma)}{d\gamma} = \frac{1}{\log 2} \log \frac{1-\gamma}{\gamma}.$$

For the function $G_\tau(\gamma) = (H(\gamma\tau) - \tau H(\gamma)) \log 2$, we have

$$\frac{dG_\tau(\gamma)}{d\gamma} = \tau \log \frac{1-\tau\gamma}{\tau\gamma} - \tau \log \frac{1-\gamma}{\gamma} = \tau \log \frac{1-\tau\gamma}{\tau-\tau\gamma} < 0.$$

Since $G_\tau(0) = 0$, the result follows. □

We repeatedly use that $\overline{\chi}(z) = \chi(z^{p-2})$ for $z \in \mathbb{F}_p^*$ and a multiplicative character χ.

We need the following statement which follows immediately from the Weil bound, see [7], and which is essentially [6, Theorem 2].

LEMMA 2. *For any multiplicative character χ modulo p of order $m \geq 2$, any integers M and K with $1 \leq K < p$, and any polynomial $F(X) \in \mathbb{F}_p[X]$ with d distinct roots (of arbitrary multiplicity) such that $F(X)$ is not the m-th power of a rational function, we have*

$$\sum_{n=M+1}^{M+K} \chi(F(n)) \ll dp^{1/2} \log p.$$

3. Multiplicative character sums

We are interested in estimates of multiplicative character sums for the sets $\mathcal{G}_s(r)$ such that 2^r is of order p and s is as small as possible.

We note that, by [1, Theorem 3], we have

$$S_s(r, \chi, f) \ll d^{1/2} \binom{r}{s}^{1/2} 2^{r/4} p^{1/8+o(1)} \tag{1}$$

(where $d = \deg f$), which provides such a nontrivial estimate (in fact even for more general sums and also with more explicit terms instead of $p^{o(1)}$).

THEOREM 1. *Let $s \le r/2$ and let χ be a nontrivial multiplicative character modulo $p > 2^r$. For any positive integers $k \le r$ and ν, and any linear polynomial $f(X) \in \mathbb{F}_p[X]$, we have*

$$|S_s(r,\chi,f)| \ll 2^{(r-k)/2\nu}\binom{r-k}{\ell}^{(\nu-1)/2\nu}\binom{r}{s}^{1/2}(\log p)^{1-1/2\nu} + 2^{k/2\nu}\binom{r}{s}^{1-1/2\nu} p^{1/4\nu}\log p,$$

where $\ell = \min\{s, \lfloor (r-k)/2 \rfloor\}$.

PROOF. Put $K = 2^{r-k}$ where $0 \le k \le r$ will be chosen later. For every $n \in \mathcal{G}_s(r)$, write $n = a2^k + b$ with $0 \le a < 2^{r-k}$ and $0 \le b < 2^k$; then

$$S_s(r,\chi,f) = \sum_{j=0}^{s} \sum_{a \in \mathcal{G}_{s-j}(r-k)} \sum_{b \in \mathcal{G}_j(k)} \chi\left(f(a2^k+b)\right).$$

By the Hölder inequality, we have

$$\begin{aligned}
|S_s(r,\chi,f)|^{2\nu} &\le (s+1)^{2\nu-1} \sum_{j=0}^{s} \binom{r-k}{s-j}^{2\nu-1} \sum_{a=0}^{K-1} \Big| \sum_{b \in \mathcal{G}_j(k)} \chi\left(f(a2^k+b)\right) \Big|^{2\nu} \\
&= (s+1)^{2\nu-1} \sum_{j=0}^{s} \binom{r-k}{s-j}^{2\nu-1} \times \\
&\quad \times \sum_{a=0}^{K-1} \sum_{\substack{b_1,\dots,b_\nu \in \mathcal{G}_j(k) \\ c_1,\dots,c_\nu \in \mathcal{G}_j(k)}} \prod_{i=1}^{\nu} \chi\left(f(a2^k+b_i)\right) \overline{\chi}\left(f(a2^k+c_i)\right) \\
&\le (s+1)^{2\nu-1} \sum_{j=0}^{s} \binom{r-k}{s-j}^{2\nu-1} \times \\
&\quad \times \sum_{\substack{b_1,\dots,b_\nu \in \mathcal{G}_j(k) \\ c_1,\dots,c_\nu \in \mathcal{G}_j(k)}} \left| \sum_{a=0}^{K-1} \prod_{i=1}^{\nu} \chi\left(f(a2^k+b_i) f(a2^k+c_i)^{p-2}\right) \right|.
\end{aligned}$$

We note that as the polynomial f is a linear polynomial over $\mathbb{F}_p$, then for any $\beta, \gamma \in \mathbb{F}_p$ with $\beta \ne \gamma$, the polynomials $f(2^kX + \beta)$ and $f(2^kX + \gamma)$ are relatively prime. In particular, these polynomials have no common roots. Now let $(b_1, \dots, b_\nu)$ and $(c_1, \dots, c_\nu)$ be two ν-tuples in $\mathcal{G}_j(k)^\nu$. We note that the function

$$\prod_{j=1}^{\nu} f(2^kX + b_j) f(2^kX + c_j)^{p-2} \tag{2}$$

is a power of another rational function whenever every value that occurs in the sequence $b_1, \dots, b_\nu$ and in the sequence $c_1, \dots, c_\nu$ occurs with a multiplicity that is at least 2. Thus, the set of such $b_1, \dots, b_\nu, c_1, \dots, c_\nu$ takes at most ν distinct values. We remark that for any subset of $G_j(k)$ with at most ν elements there are at most

$$\binom{k}{j} + \binom{k}{j}^2 + \cdots + \binom{k}{j}^\nu \le 2\binom{k}{j}^\nu$$

possibilities. When such a subset with $k \le \nu$ elements is fixed, we can obtain the case described above by placing its elements into 2ν positions. This can be done in no more than $(2\nu)^k \le (2\nu)^\nu$ ways. So we have at most $2(2\nu)^\nu \binom{k}{j}^\nu$ possibilities for vectors $(b_1, \dots, b_\nu)$ and $(c_1, \dots, c_\nu)$ such that the function (2) is a power of another rational function. Using now Lemma 2 when the rational function (2) is not a power of another rational function, we can estimate

$$\sum_{\substack{b_1,\dots,b_\nu \in \mathcal{G}_j(k) \\ c_1,\dots,c_\nu \in \mathcal{G}_j(k)}} \Big| \sum_{a=0}^{K-1} \prod_{i=1}^{\nu} \chi\left(f(a2^k + b_i) f(a2^k + c_i)^{p-2}\right) \Big|$$

$$\ll \binom{k}{j}^\nu K + \binom{k}{j}^{2\nu} p^{1/2} \log p = \binom{k}{j}^\nu 2^{r-k} + \binom{k}{j}^{2\nu} p^{1/2} \log p.$$

Therefore,

$$S_s(r, \chi, f)^{2\nu} \ll s^{2\nu-1} \Sigma_1 2^{r-k} + s^{2\nu-1} \Sigma_2 p^{1/2} \log p, \tag{3}$$

where

$$\Sigma_1 = \sum_{j=0}^{s} \binom{r-k}{s-j}^{2\nu-1} \binom{k}{j}^\nu,$$

$$\Sigma_2 = \sum_{j=0}^{s} \binom{r-k}{s-j}^{2\nu-1} \binom{k}{j}^{2\nu}.$$

Clearly,

$$\binom{r-k}{s-j} \le \max\left\{ \binom{r-k}{s}, \binom{r-k}{\lfloor (r-k)/2 \rfloor} \right\} = \binom{r-k}{\ell}.$$

From the identity

$$\sum_{j=0}^{s} \binom{r-k}{s-j} \binom{k}{j} = \binom{r}{s},$$

we see that

$$\Sigma_1 \le \binom{r-k}{\ell}^{\nu-1} \sum_{j=0}^{s} \binom{r-k}{s-j}^\nu \binom{k}{j}^\nu$$

$$\le \binom{r-k}{\ell}^{\nu-1} \left(\sum_{j=0}^{s} \binom{r-k}{s-j} \binom{k}{j} \right)^\nu = \binom{r-k}{\ell}^{\nu-1} \binom{r}{s}^\nu.$$

Since $\binom{k}{j} \le 2^k$, we also obtain

$$\Sigma_2 \le 2^k \sum_{j=0}^{s} \binom{r-k}{s-j}^{2\nu-1} \binom{k}{j}^{2\nu-1} \le 2^k \left(\sum_{j=0}^{s} \binom{r-k}{s-j} \binom{k}{j} \right)^{2\nu-1} = 2^k \binom{r}{s}^{2\nu-1}.$$

Thus, we derive from (3) that

$$S_s(r,\chi,f)^{2\nu} \ll s^{2\nu-1} \left(2^{r-k} \binom{r-k}{\ell}^{\nu-1} \binom{r}{s}^{\nu} + 2^k \binom{r}{s}^{2\nu-1} p^{1/2} \log p \right).$$

Since $s \ll r \ll \log p$ we obtain the desired result.

□

Taking $\nu = 1$ and defining k by the inequalities

$$2^k \le 2^{r/2} p^{-1/4} (\log p)^{1/2} < 2^{k+1},$$

we see that the bound in Theorem 1 becomes of the same form as (1).

Clearly, if $2^r = p^{1+o(1)}$ then provided that $r/2 \ge s \ge \gamma r$ the bound (1) is nontrivial for any constant $\gamma > \vartheta_0$ where $\vartheta_0 = 0.2145017449\ldots$ is the root of the equation

$$H(\vartheta) = 3/4, \qquad 0 \le \vartheta \le 1/2.$$

We now show that if 2^r is of order p, than Theorem 1 provides a nontrivial bound for $r/2 \ge s \ge \gamma r$ for any constant $\gamma > \rho_0$ where $\rho_0 = 0.11002786\ldots$ is the root of the equation

$$H(\rho) = 1/2, \qquad 0 \le \rho \le 1/2. \tag{4}$$

THEOREM 2. *For any $\gamma > \rho_0$, where $\rho_0 = 0.11002786\ldots$ is the root of equation (4), there exists some $\eta > 0$ such that if $p > 2^r = p^{1+o(1)}$ and $r/2 \ge s \ge \gamma r$, then for any nontrivial multiplicative character χ modulo p, we have*

$$S_s(r,\chi,f) \ll \binom{r}{s}^{1-\eta}.$$

PROOF. We may assume that $\gamma < 1/2$ as otherwise the bound (1) implies the desired result.

We put $k = \lfloor \kappa r \rfloor$, where

$$\kappa = \min \left\{ \frac{1-2\gamma}{2}, \frac{2H(\gamma)-1}{4} \right\}.$$

Using that $\kappa \le 1/2 - \gamma$ we derive $k \le r - 2s$, thus $\ell = s$, and the bound of Theorem 1 implies that

$$|S_s(r,\chi,f)| \le 2^{\alpha r + o(r)} + 2^{\beta r + o(r)},$$

where

$$\alpha = \frac{1}{2\nu}(1-\kappa) + \frac{\nu-1}{2\nu} H\Big(\frac{\gamma}{1-\kappa}\Big)(1-\kappa) + \frac{1}{2}H(\gamma),$$
$$\beta = \frac{1}{2\nu}\kappa + \frac{2\nu-1}{2\nu}H(\gamma) + \frac{1}{4\nu}.$$

Clearly

$$\alpha < \frac{1}{2\nu}(1-\kappa) + \frac{1}{2}\Big(H\Big(\frac{\gamma}{1-\kappa}\Big)(1-\kappa) + H(\gamma)\Big).$$

Since $\gamma/(1-\kappa) < 2\gamma < 1$, by Lemma 1 we have

$$H\Big(\frac{\gamma}{1-\kappa}\Big)(1-\kappa) < H(\gamma).$$

So, choosing a sufficiently large ν to satisfy

$$\frac{1-\kappa}{2\nu} < \frac{H(\gamma)}{2} - H\Big(\frac{\gamma}{1-\kappa}\Big)(1-\kappa)$$

we achieve $\alpha < H(\gamma)$.

Furthermore, using that $\kappa \le (2H(\gamma)-1)/4$, we also have

$$\beta \le \frac{2H(\gamma)-1}{8\nu} + \frac{H(\gamma)(2\nu-1)}{2\nu} + \frac{1}{4\nu} = H(\gamma) - \frac{H(\gamma)}{4\nu} + \frac{1}{8\nu}.$$

Since $H(\gamma) > H(\rho_0) = 1/2$, we see that $\beta < H(\gamma)$. Taking

$$\eta = 1 - \frac{\min\{\alpha,\beta\}}{H(\gamma)} > 0$$

we conclude the proof. □

4. Applications

We now show how Theorems 1 and 2 can be used to study the distribution of products $n_1 \dots n_m$ with $n_1, \dots, n_m \in \mathcal{G}_s(r)$ in residue classes modulo p. Let $N_{s,m}(r,\lambda)$ denote the number of solutions to the congruence

$$n_1 \cdots n_m \equiv \lambda \pmod p, \qquad n_1, \dots, n_m \in \mathcal{G}_s(r). \tag{5}$$

We present only one result out of the variety of many other results of this type which can be derived from Theorems 1 and 2 in a similar fashion.

THEOREM 3. *For any $\gamma > \rho_0$, where $\rho_0 = 0.11002786\ldots$ is the root of equation (4), there exist some m_0 and $\xi > 0$ such that if $p > 2^r = p^{1+o(1)}$ and $r/2 \ge s \ge \gamma r$, then for $m \ge m_0$ we have*

$$N_{s,m}(r,\lambda) = \frac{1}{p-1}\binom{r}{s}^m \big(1 + O(p^{-\xi m})\big)$$

uniformly over all integers $\lambda \not\equiv 0 \pmod p$.

PROOF. We recall the following orthogonality relation for multiplicative character sums:

$$\frac{1}{p-1}\sum_{\chi} \chi(u)\overline{\chi(\lambda)} = \begin{cases} 1, & \text{if } u = \lambda, \\ 0, & \text{if } u \ne \lambda, \end{cases}$$

where the sum is taken over all multiplicative characters of $\mathbb{F}_p^*$.

Therefore, for any integer λ, the number of solutions to the congruence (5) can be written as

$$\begin{aligned} N_{s,m}(r,\lambda) &= \frac{1}{p-1} \sum_{n_1,\ldots,n_m \in \mathcal{G}_s(r)} \sum_{\chi} \chi(n_1 n_2 \ldots n_m)\overline{\chi(\lambda)} \\ &= \frac{1}{p-1} \sum_{\chi} \overline{\chi(\lambda)} \sum_{n_1,\ldots,n_m \in \mathcal{G}_s(r)} \chi(n_1 n_2 \ldots n_m) \\ &= \frac{1}{p-1} \sum_{\chi} \overline{\chi(\lambda)} \Big(\sum_{n \in \mathcal{G}_s(r)} \chi(n) \Big)^m, \end{aligned}$$

where the sum is taken over all multiplicative characters of $\mathbb{F}_p^*$.

Separating the term

$$\frac{1}{p-1}\#\mathcal{G}_s(r)^m = \frac{1}{p-1}\binom{r}{s}^m$$

corresponding to the trivial character χ_0 we obtain

$$N_{s,m}(r,\lambda) - \frac{1}{p-1}\binom{r}{s}^m \ll \frac{1}{p-1}\sum_{\chi} \Big| \sum_{n \in \mathcal{G}_s(r)} \chi(n) \Big|^m.$$

Applying the bound of Theorem 2 and the fact that the order of the group of multiplicative characters of $\mathbb{F}_p^*$ is $p-1$, it follows that there exists some $\eta > 0$ such that we get the estimate

$$N_{s,m}(r,\lambda) - \frac{1}{p-1}\binom{r}{s}^m \ll \binom{r}{s}^{m-m\eta},$$

and thus

$$N_{s,m}(r,\lambda) = \frac{1}{p-1}\binom{r}{s}^m \left(1 + O\left(p\binom{r}{s}^{-m\eta}\right)\right).$$

As

$$H(s/r) > 1/2 \qquad \text{and} \qquad 2^r = p^{1+o(1)},$$

we obtain that

$$p\binom{r}{s}^{-m\eta} = p2^{-m\eta(rH(s/r)+o(r))} \le p^{1-m\eta/2+o(1)}.$$

Taking now $\xi = \eta/3 > 0$ we see that for a sufficiently large $m \ge m_0$, we have the desired result.

□

Acknowledgement

The authors are grateful to Jung Hee Cheon who attracted their attention to the problems considered in this work and their cryptographic relevance. These conversations took place at the CRM (Montréal) Workshop on Computer Security and Cryptography, 12–16 April, 2010; the generous support and hospitality of the CRM are greatly appreciated.

During the preparation of this paper, the first author was supported in part by SNF Grant 121874 (Switzerland) and the second author by ARC Grant DP1092835 (Australia) and by NRF Grant CRP2-2007-03 (Singapore).

References

[1] W. Banks, A. Conflitti and I. E. Shparlinski, Character sums over integers with restricted g-ary digits, *Illinois J. Math.*, **46** (2002), 819–836.

[2] J. H. Cheon, S. Jarecki, T. Kwon and M.-K. Lee, Fast exponentiation using split exponents, *IEEE Trans. on Inform. Theory*, to appear.

[3] J. B. Friedlander and I. E. Shparlinski, On the distribution of Diffie–Hellman triples with sparse exponents, *SIAM J. Discrete Math.*, **14** (2001), 162–169.

[4] J. Hoffstein and J. Silverman, Random small Hamming weight products with applications to cryptography, *Discrete Appl. Math.*, **130** (2003), 37–49.

[5] F. J. MacWilliams and N. J. A. Sloane, *The Theory of Error-Correcting Codes*, North-Holland, Amsterdam, 1977.

[6] C. Mauduit and A. Sárközy, On finite pseudorandom binary sequences 1: Measure of pseudorandomness, the Legendre symbol, *Acta Arith.*, **82** (1997), 365–377.

[7] A. Weil, *Basic number theory*, Springer-Verlag, New York, 1974.